July 6th, 2016
Chairman Tom Wheeler
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Chairman Wheeler:

The Internet Keep Safe Coalition (iKeepSafe), is an international alliance of more than 100 policy leaders, educators, law enforcement members, technology experts, public health experts and advocates. iKeepSafe's Board of Directors includes nationally recognized thought leaders in online privacy, security, ethics, law, health, and safety. We track global trends and issues surrounding digitally connected products and their effect on children. This research drives the continuous creation of positive resources for parents, educators and policymakers to teach children how to use new technologies and the Internet in safe and healthy ways. We also work with industry, education, government and policy leaders to explore concerns related to online privacy, security, safety and compliance and create resources to address those concerns.

iKeepSafe's partnerships are integral to the success and scale of our research and programs. iKeepSafe engages with industry and government, joining national and international advisory boards specifically addressing child privacy, safety, security and health. We collaborate with international organizations such as the United Nations Children's Emergency Fund (UNICEF), International Technological University (ITU), the United Nations Educational, Scientific, and Cultural Organization (UNESCO) and the Internet Governance Forum (IGF). National organization partners include the Federal Trade Commission, the National Telecommunications and Information Administration, the Internet Safety Technical Task Force, the National Institute of Standards and Technology (NIST), and the National Cyber Security Alliance. Our industry partners include Comcast, Verizon, AT&T, Symantec, Google, Kaspersky, ASKfm, Twitter, Facebook, Snapchat, Yahoo, Adobe, AOL, Cisco, and others.

Privacy and Information Security Are at the Core of Everything We Do

iKeepSafe understands the importance of online privacy. Our mission is to give parents, educators, and policymakers information and tools which empower them to teach our children the safe and healthy use of technology and the Internet. We are a recognized leader in privacy education. We created the first comprehensive K-12 privacy curriculum — the *Privacy K-12 Curriculum Matrix* — enabling educators to develop a cohesive approach to teaching students both why and how to protect personal information[1]. We also developed the first comprehensive privacy guide for K-12 school systems — *Digital Compliance and Student Privacy: A Roadmap for Schools*[2]. Additionally, we created and implemented the first FERPA and state student data

[1] http://ikeepsafe.org/privacy-k-12-curriculum-matrix/
[2] http://ikeepsafe.org/educators_old/digital-compliance-and-student-privacy-a-roadmap-for-schools/

privacy assessments for edtech vendors to help educators find and use products that protect student information[3]. Our *Digital Privacy, Safety and Security* self-assessment module for schools helps them identify and measure their own data governance and practices[4]. Through these and other initiatives, we work with both industry and educators to go above and beyond legal requirements by fostering a positive digital culture — an environment where youth can thrive using technology.

This includes partnering with Internet Service Providers (ISPs) and schools to promote the importance of privacy, security and online reputation to students nationwide. iKeepSafe periodically meets with Comcast's business and legal teams to discuss the latest developments and technology regarding protecting consumer data and empowering consumers, particularly parents and children. Our "Project PRO (Privacy and Reputation Online)," created in partnership with the American School Counselor Association (ASCA) and AT&T, is an interactive program promoting the importance of security and reputation to students nationwide[5]. We also work with ISPs such as Verizon and Comcast to create and distribute educational content to parents, educational institutions and cable stations nationwide. Our experience with our ISP partners is that they value the relationship with their customers, and strive to educate their users — especially children — about the importance of online safety and privacy protection.

Parents and Students Need a Consistent Framework

iKeepSafe's primary goal is to keep children safe online. To accomplish this, we provide educational resources to parents that help them keep up-to-date with new technology, including the way information is collected, used and shared across the Internet Ecosystem. Our core message to parents is: "You Don't Have to Be a Computer Expert to Keep Your Child Safe Online." However, the FCC's proposed privacy rules have the potential to undermine that message by making privacy and data security on the Internet seem far more complicated.

Currently, our educational resources are based on legal regimes that offer an approach that is inconsistent with the FCC's proposed rules for broadband privacy. As privacy advocates, educators, and an FTC safe harbor, iKeepSafe welcomes privacy efforts that increase transparency, consistency, and capacity for consumers to better manage their digital privacy. Unfortunately, the FCC's proposed rules for broadband privacy create inconsistent protection and expectations. As the FTC articulates, "the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of BIAS services that would not generally apply to other services that collect and use significant amounts of consumer data."[6] In fact, we believe such an approach will result in significant consumer confusion, over-notification, and ultimately *less* privacy and security for consumers overall. Consumers without significant technology backgrounds will likely misunderstand the limitations of the protections, and may even make assumptions that potentially put themselves at greater risk. As the FCC moves forward to finalize its rules for broadband privacy, we urge you to remain aligned with existing legal regimes and offer consumers consistent and meaningful privacy protections and choices.

The FCC has proposed a privacy regime for ISPs that would result in rules that are inconsistent

---

[3] http://ikeepsafe.org/privacy
[4] http://digitalprivacy.brightbytes.net/
[5] http://ikeepsafe.org/parents/project-pro/
[6] Federal Trade Commission. Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission. Page 8.
https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf

with the privacy obligations applied to the rest of the Internet Ecosystem. The new rules would require varying levels of notice, choice, and security based on the fact that information is collected and used by a particular type of entity, rather than the sensitivity of the information. Although we appreciate the FCC's commitment to privacy, we agree with the FTC that having a different set of rules governing the same exact information is "not optimal" for consumers. In fact, such disparate treatment of the same exact information by different entities will cause confusion among consumers. A recent study by the Progressive Policy Institute found that **94%** of Internet users surveyed "strongly agree that all companies collecting data online should follow the same consumer privacy rules." Additionally, there is no evidence that the use of what has been historically considered "non-sensitive" data requires a heightened level of consent; **83%** of those Internet users surveyed said their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data. The results of this survey are consistent with existing privacy and information security laws, as well as FTC staff's comments to the FCC in this docket.

In the course of preparing our programs and working with our diverse constituents, we come across many forms of data that are governed by just as many laws and regulations. What each of these legal regimes has in common is the underlying premise that some data – such as personal health information, children's data, or data about students – are certainly more sensitive than others, and imposing heightened requirements on collection, use, and sharing of this data is important. Because privacy is often subjective and based on the individual consumer's preferences, there are other types of information that may be sensitive to some, but not to others. In these instances, notice of collection, use, and disclosure is still appropriate, and consumers have the ability to restrict certain uses and disclosures. We educate parents and students about these choices to put them in control of their online information and experience.

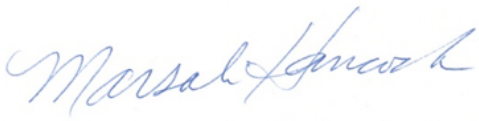
iKeepSafe agrees that there may be instances where heightened notice and consent requirements are helpful. The FCC proposes that its regulations would cover any data that is "linked or linkable" to an individual. This broad scope would likely include every piece of information that is even remotely connected to an individual. Broadband service providers would be required to obtain a consumer's "opt-in" consent to use this information for the vast majority of purposes, and would even be required to offer "opt-out" or "opt-in" choices to consumers for use of aggregated or de-identified information. If adopted as such, we fear consumers will be barraged with requests for the use of non-sensitive information, causing confusion or worse – desensitizing consumers in a way that results in rote consent to (or rejection of) every request received. Likewise, we are concerned that multi-layered rules would result in more complex and complicated privacy policies, overwhelming consumers who may, as a result, be less likely to consult and fully review these important guidelines.

We have similar concerns with respect to the Commission's proposed breach notification requirements. For example, the FCC's proposal would require broadband service providers to notify consumers when information is accessed by an employee in good faith, or when the information at issue is encrypted, resulting in no harm to the consumer. The proposed rules would also require consumer notification if a list of IP addresses was inadvertently accessed or shared, even if no other information was associated with this list, regardless of the fact that this information is publicly available through online directories such as whois.com, and regardless of the fact that the broadband service provider may have to collect *additional information they might not have otherwise collected* – such as an email address – to ensure that they can send notifications in case of a breach. Studies indicate that nearly a third of consumers already do nothing when they receive breach notifications that actually involve information that can lead to

financial harm or identity theft. Under the proposed rules, we anticipate breach notifications would increase to the point that consumers would simply disregard them, and thus miss the important notifications of breaches that could result in real harm to the consumer or their family. This concern was shared by the FTC in its comments, along with the concern that such broad notification requirements may harm consumers in other ways, including requiring the collection and retention of more information than would otherwise be necessary.

In light of these concerns, we urge you to revise the proposed approach and fashion rules to protect consumer information that is truly sensitive and that, if inappropriately used or disclosed, could result in serious harm to those consumers. This time-tested approach is not only consistent with existing privacy regimes, but will also better enable consumers to more easily understand how their information is being used throughout the Internet Ecosystem and make meaningful choices. Introducing varying standards and voluminous consumer notices, will cause confusion and may ultimately result in consumers taking *fewer* steps to understand and protect their privacy.

Sincerely,



Marsali Hancock

President and CEO, iKeepSafe